DXi-Series Configuration and Best Practices Guide Generating and Deploying TLS Certificates

Contents

Certificate Generation Using a Certification Authority (CA)

Step 1: Generate Private Key

Generate a private key to be used for creating the Certificate Signing Request (CSR):

```
$ openssl genrsa -out key.pem 2048
```

Step 2: Generate Certificate Signing Request (CSR)

Generate a CSR using the private key. Ensure that the Common Name (CN) in the CSR matches the hostname of your server:

```
$ openssl req -new -key key.pem -out csr.pem -subj
"/C=IN/ST=KA/L=bangalore/O=quantum/CN=server-1/emailAddress=test@quantum.com"
```

Note:

- The CSR includes the public key and information such as the server's hostname, organization, and country.
- Verify that the CN field corresponds to the hostname of the server.

Step 3: Submit CSR to the Certificate Authority (CA)

Provide the generated csr.pem file to your Certificate Authority for signing. The CA will issue a signed certificate (e.g., cert.pem) and may also provide intermediate certificates.

Full Certificate Chain Requirement:

- The ROOT CA need to be combined with all intermediate certificates provided by the CA into a full certificate chain.
- Example of a chained CA certificate file (cacert.pem):

  ```
  -----BEGIN CERTIFICATE-----
  ROOT CA cert
  -----END CERTIFICATE-----
  -----BEGIN CERTIFICATE-----
  SUB CA cert
  -----END CERTIFICATE-----
  ```

Note: The order of certificates in the chain can sometimes affect the validation process. Ensure the Root CA is at the top, followed by intermediate CAs in hierarchical order.

Step 4: Validate the Signed Certificate

Once you receive the signed certificate (cert.pem), verify it against the full CA certificate chain:

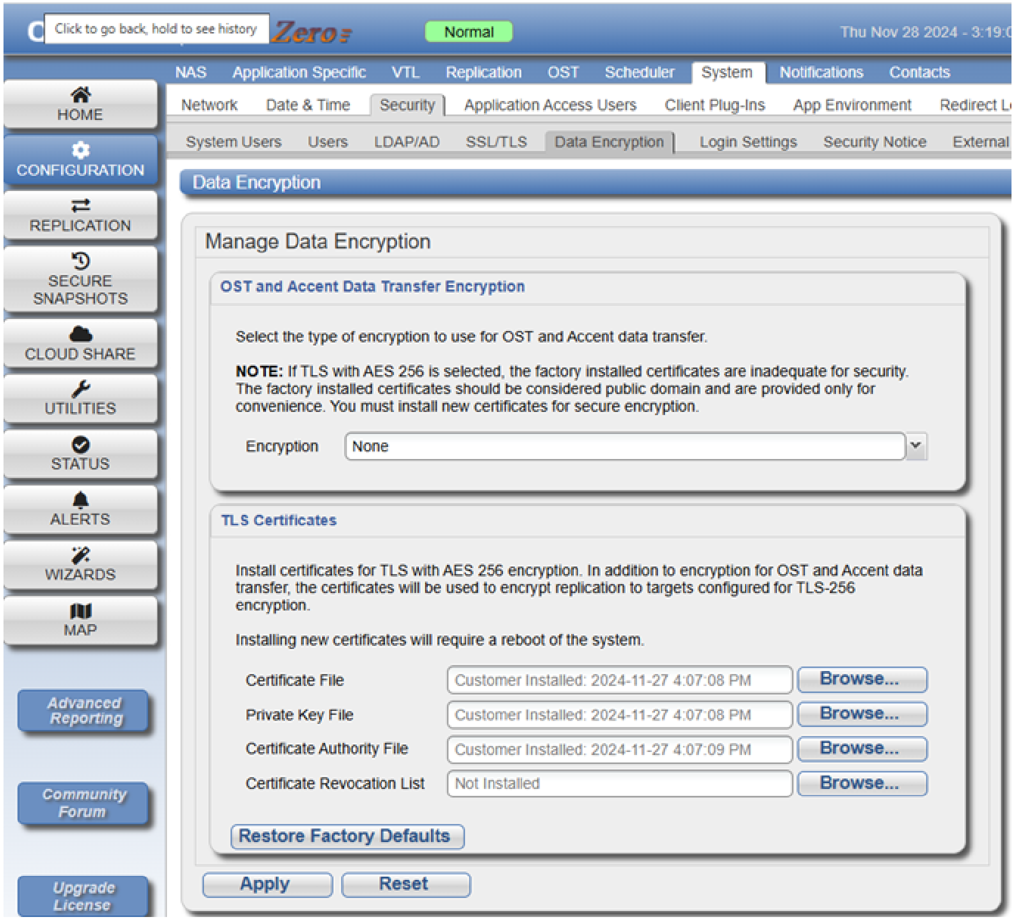
```
$ openssl verify -CAfile cacert.pem cert.pem
cert.pem: OK
```

Note: If validation fails, check that the full certificate chain is correct and in the appropriate order.

Step 5: Deploy the Certificates

Upload the following files to the server in TLS Certificates section:

1. **Certificate File** (Signed Certificate - cert.pem)
2. **Private Key File** (key.pem)
3. **Certificate Authority File** (Full Certificate Chain - cacert.pem)



Data Encryption

Manage Data Encryption

OST and Accent Data Transfer Encryption

Select the type of encryption to use for OST and Accent data transfer.

NOTE: If TLS with AES 256 is selected, the factory installed certificates are inadequate for security. The factory installed certificates should be considered public domain and are provided only for convenience. You must install new certificates for secure encryption.

Encryption: None

TLS Certificates

Install certificates for TLS with AES 256 encryption. In addition to encryption for OST and Accent data transfer, the certificates will be used to encrypt replication to targets configured for TLS-256 encryption.

Installing new certificates will require a reboot of the system.

Certificate File	Customer Installed: 2024-11-27 4:07:08 PM
Private Key File	Customer Installed: 2024-11-27 4:07:08 PM
Certificate Authority File	Customer Installed: 2024-11-27 4:07:09 PM
Certificate Revocation List	Not Installed

Additional Notes

Order of Certificates in cacert.pem:

- The order can matter in some implementations. Ensure the Root CA is first, followed by intermediate CAs in order of hierarchy.
- If validation fails, try reordering the certificates in cacert.pem and test again.

Common Errors:

- Validation may fail if the full chain is incomplete

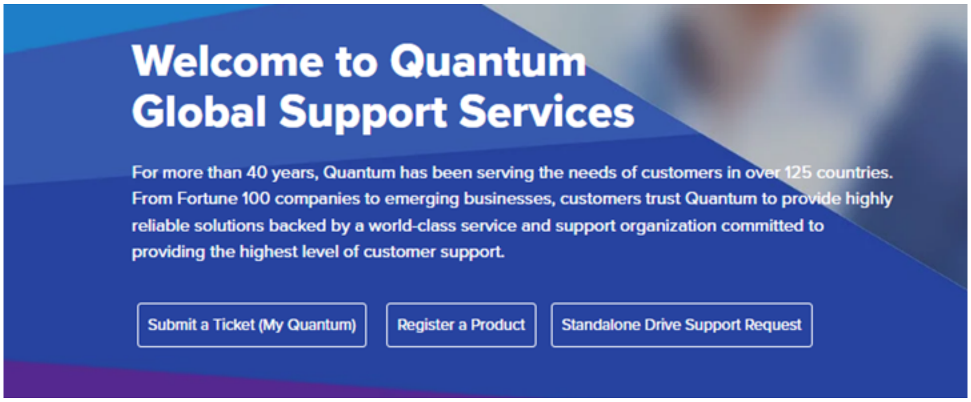
Contacting Quantum Support

Below is information related to contacting Quantum Support as well as steps to improve your Quantum customer journey.

- Submit a Ticket (Service Request) below
- Use MyQuantum Service Delivery Platform on the next page
- Use Cloud Based Analytics (CBA) on page 6
- Escalate a Case on page 6
- Contact Quantum Sales on page 6

Submit a Ticket (Service Request)

If you need to submit a ticket or speak to Quantum technical support, go to the Support page at https://www.quantum.com/en/service-support/

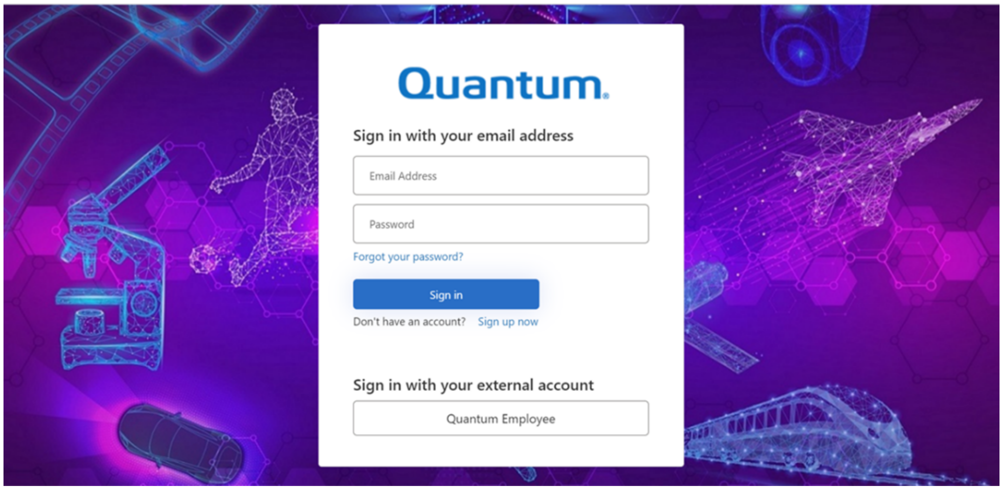


Welcome to Quantum Global Support Services

For more than 40 years, Quantum has been serving the needs of customers in over 125 countries. From Fortune 100 companies to emerging businesses, customers trust Quantum to provide highly reliable solutions backed by a world-class service and support organization committed to providing the highest level of customer support.

Submit a Ticket (My Quantum)
Register a Product
Standalone Drive Support Request

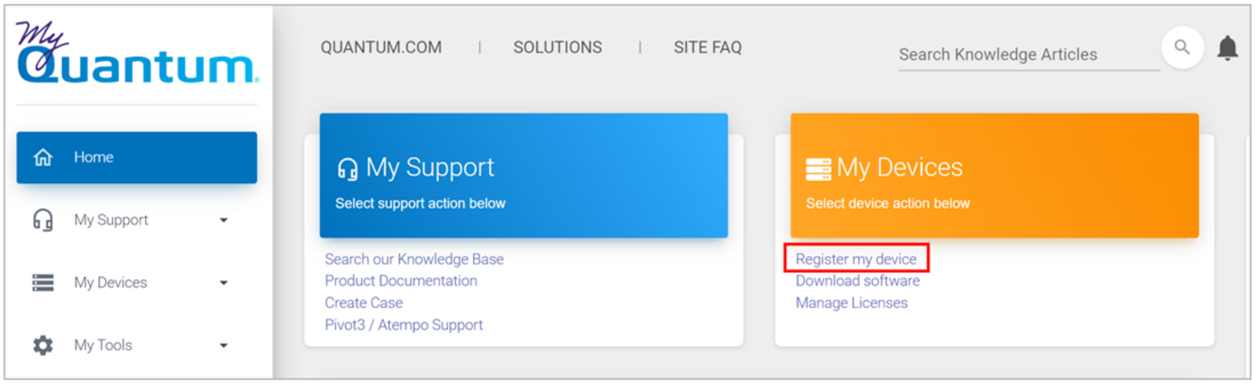
To start the process with Quantum Technical Support, click **Submit a Ticket**. From here, sign in to the MyQuantum Service Delivery Platform or create an account. For more information, refer to the Use MyQuantum Service Delivery Platform below section below.


Quantum.
Sign in with your email address
Email Address
Password
Forgot your password?
Sign in
Don't have an account? Sign up now
Sign in with your external account
Quantum Employee

Use MyQuantum Service Delivery Platform

MyQuantum is a single portal for everything Quantum. You can view assets, open support cases, receive real-time updates, and search the Knowledge Base and documentation, all through a secure, online portal.

1. Create an account and log in to the MyQuantum Service Delivery Platform.
2. Register a product on MyQuantum.



3. Request site access to the Cloud-Based Analytics (CBA) monitoring portal and follow the instructions to set up product(s) to connect to CBA. You can use CBA to monitor Quantum products remotely, from a single dashboard, and Quantum Support can use it to help troubleshoot products more efficiently.

Refer to product documentation for product-specific information related to CBA.

Use Cloud Based Analytics (CBA)

Quantum products are equipped with a Cloud Based Analytics (CBA) agent that can provide log files and snapshots to Quantum CBA servers that are running in the cloud.

CBA enables Quantum systems to collect data regarding system and environment performance. The collected data is bundled and uploaded to the remote CBA server for analysis. You can access Quantum system performance and health results on the CBA dashboard (at https://insight.quantum.com) or through the MyQuantum Service Delivery Platform.

The CBA dashboard displays the analytic results of the uploaded CBA data using flexible charting tools, along with an overall health score of each Quantum system configured for the CBA account.

Escalate a Case

To escalate a case, follow the process documented here: https://www.quantum.com/en/service-support/resources/escalation/

Contact Quantum Sales

https://www.quantum.com/en/company/contact-us/